Cutting Through SIEM Vendor Marketing

Make the right technology decision

A. Ananth

ananth@eventtracker.com

Outline

- What's in a name? SIEM? SEM? SIM?
- Customer Motivations
- Vendor approaches to the problem
- Deciding what's right for you
- Worst practices
- Q&A

What's in a name?

- SIEM – Gartner's name for this space, Includes support for:
  - SIM – Log management and compliance reporting (non realtime tasks)
  - SEM – Incident management for security related events (realtime task)
- Ops use case is increasingly important
  - Tighter budgets
  - Strong benefits

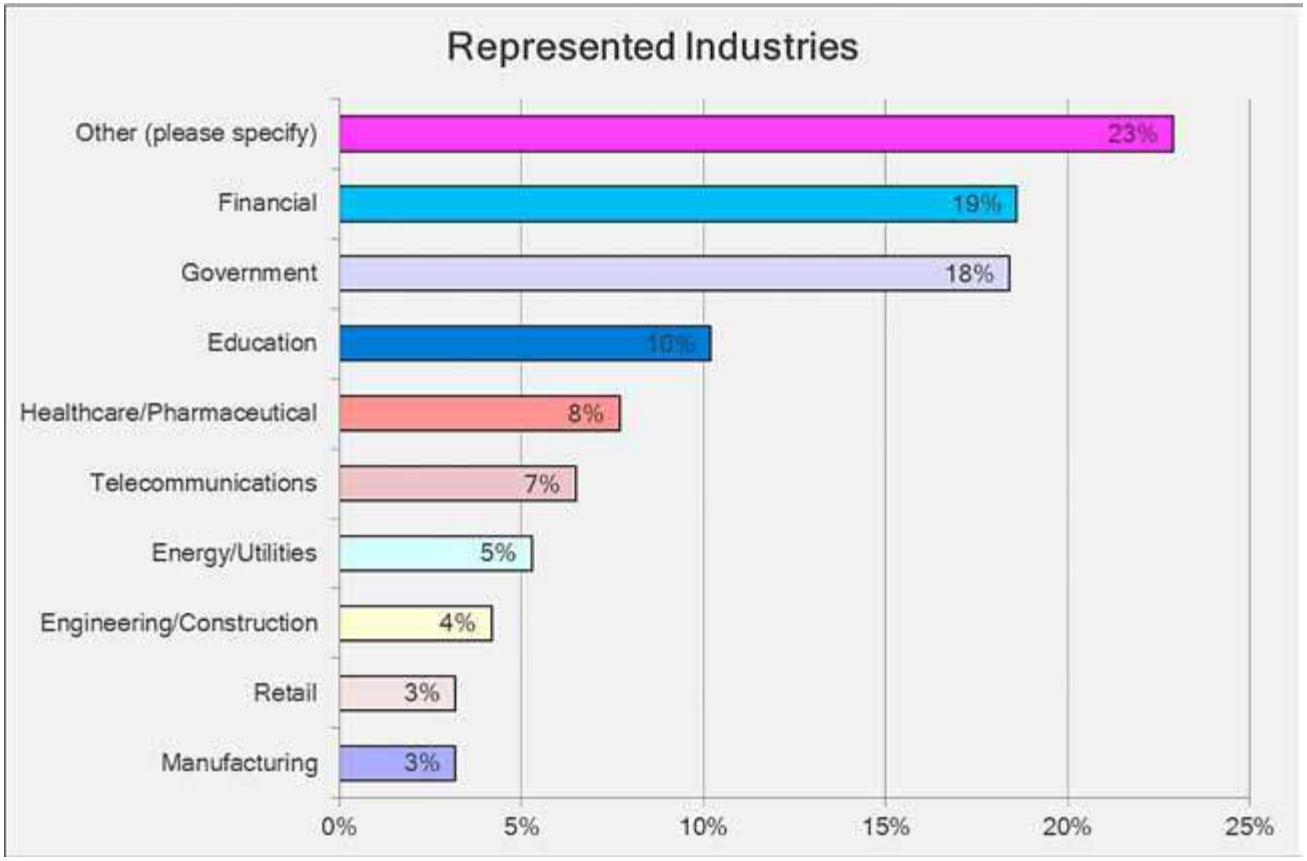
Customer motivations

- Help, I'm being audited!
  - Compliance reporting
- Help, I'm being hacked!
  - Threat management
- Help, I'm being RIF'ed
  - More with less
- Help, I want to comply with "best practice"
  - Just checking if you are still awake

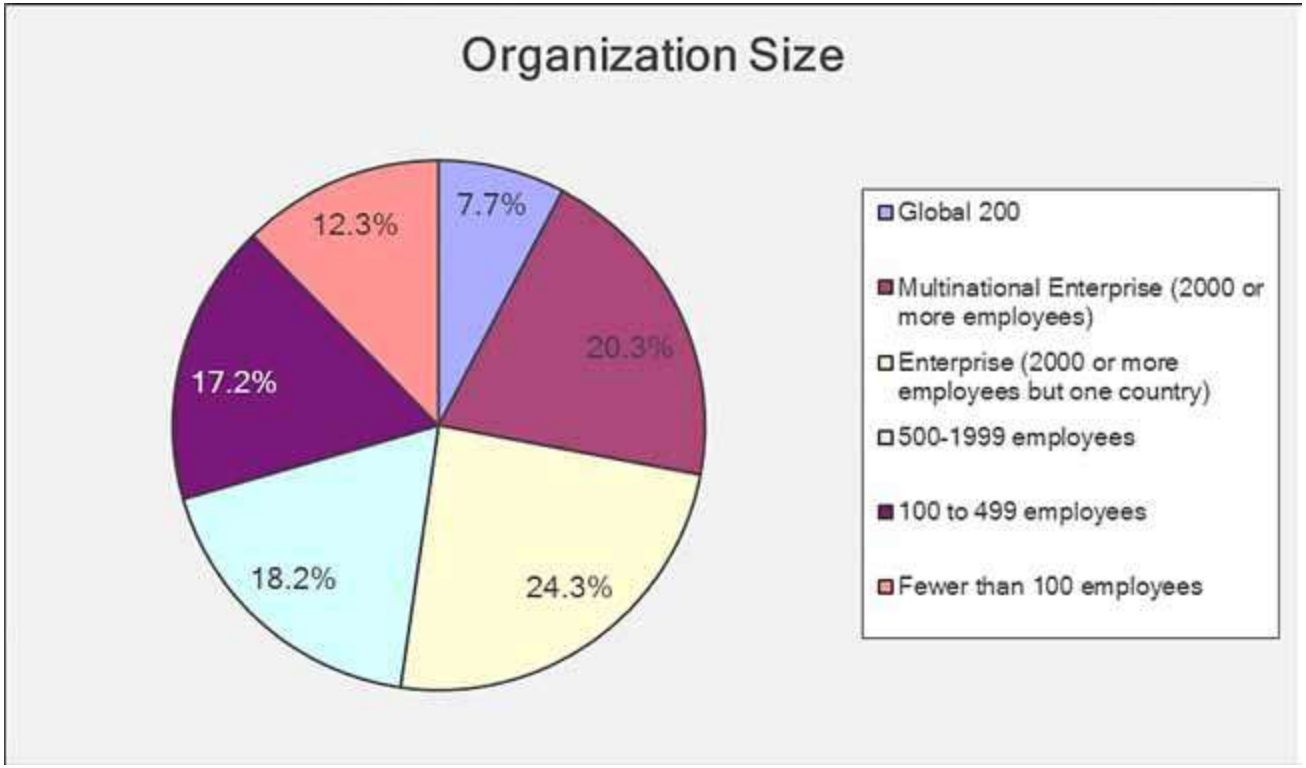
Evolution 2005-2011

- SANS Annual Log Management survey
  - 2005: 43% of those surveyed collected logs
  - 2011: 89% of those surveyed collected logs
    - More data from physical/plant/POS devices

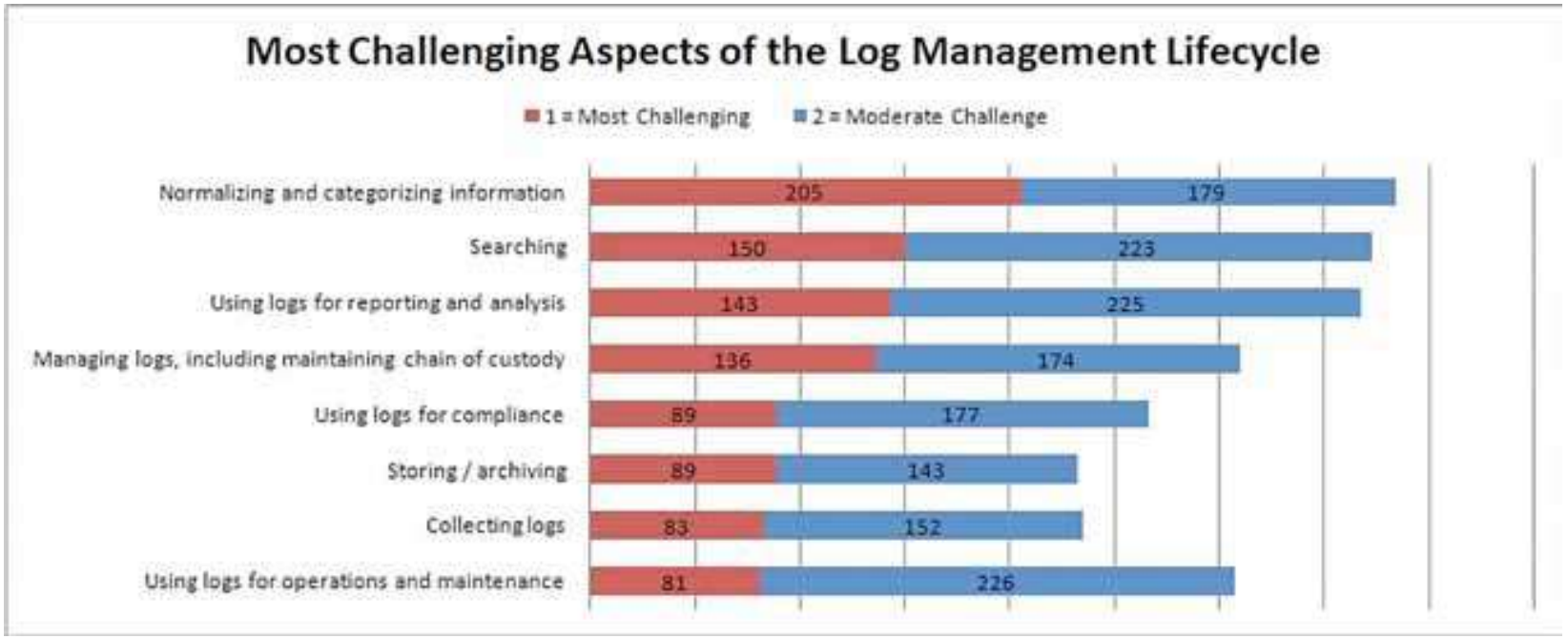
Which verticals?



Company size



What is difficult?



What is difficult?

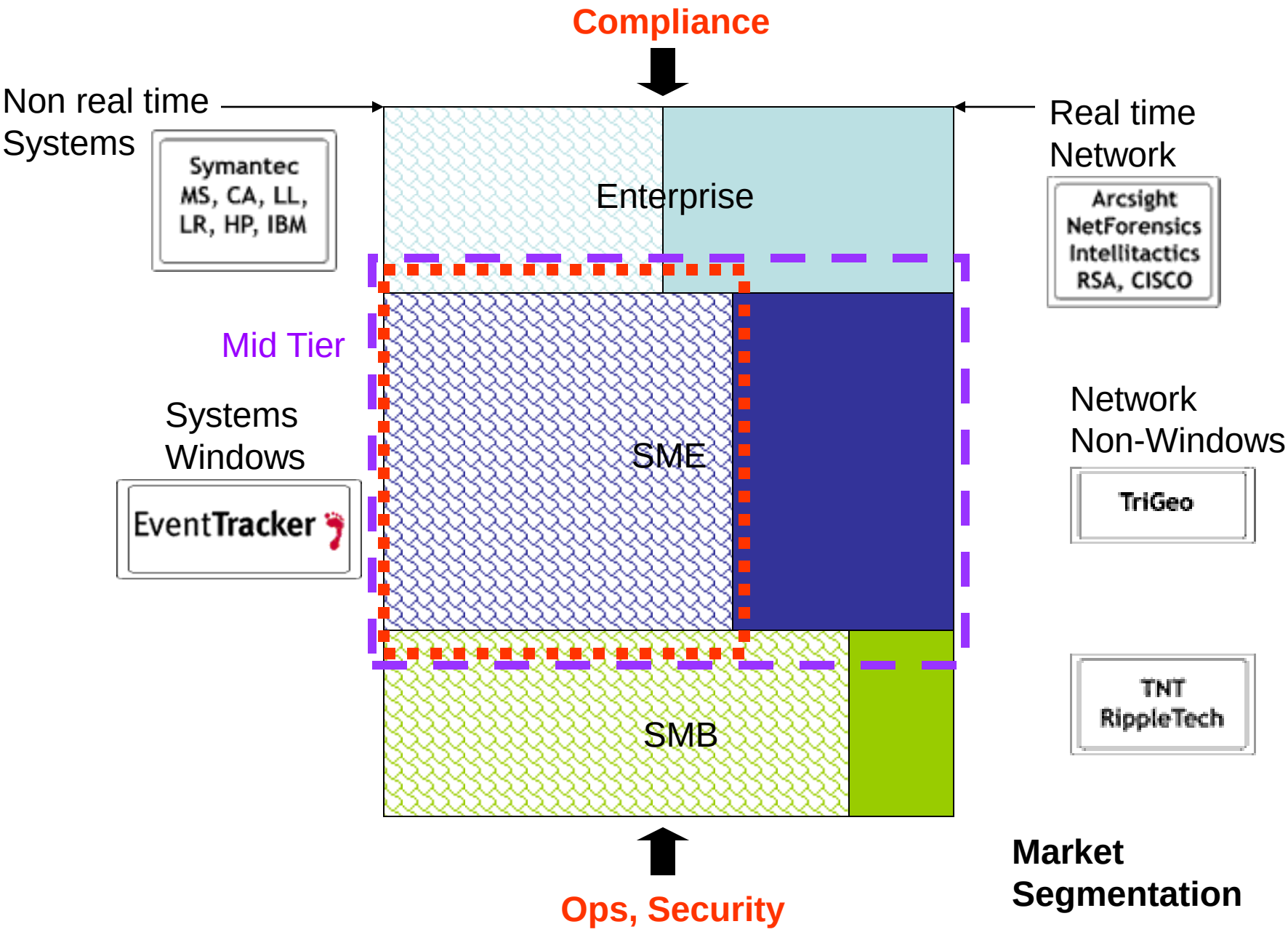
- The mechanics of collecting, storing and archiving the log data are no longer the challenge
- The challenge now is extracting the needed information for monitoring, mgt, compliance and decision-making (often in near real-time)
- Windows logs remain a challenge

Vendor approaches

- SEM is the “real” problem
  - Focused on the SOC
  - The network is the computer
  - “Correlation is it”
- SIM is the “real” problem
  - Focused on archival
  - Compliance reporting

Vendor approaches

- Normalization is the key
  - Parsers, standard SQL schema
  - Ever larger ODBC instances
  - Vendor “standards”
- Vulnerability is the key
  - Huh?
- Netflow/Jflow is the key
  - Another “network” based approach


Compliance
Non real time
Systems
Symantec
MS, CA, LL,
LR, HP, IBM
Enterprise
Real time
Network
Arcsight
NetForensics
Intellitactics
RSA, CISCO
Mid Tier
Systems
Windows
EventTracker
SME
Network
Non-Windows
TriGeo
SMB
TNT
RippleTech
Ops, Security
Market
Segmentation

Deciding what's right for you

- Start with the real reason
  - Monitor for PCI-DSS, protect web apps
  - Monitor critical servers for suspicious login
- Include log sources
- Size the environment
  - Consider phased approach

Deciding what is right for you

- Describe essential SIEM features
  - Which reports/trends, role based dashboards, Netflow, Change monitoring, search etc
  - SEM? SIM? Ops?
- Keep it short
  - More than 10 pages? Go back and prune

SIEM Mythology

- Auto learning, no tuning required
  - Like the “self driving” car aka pink elephant
- Analyst-in-a-box
  - Think “virtual box for the analyst”
- Minimal or no training needed
  - A fool with a tool is still a fool
- SIEM is scientific
  - More like art with politics on the side

SIEM Project lifecycle

- Determine the need
- Define scope
- Make shortlist of vendors
- Conduct POC
- Deploy
- Use
- Expand

Worst practices

- Determine need: Skip this step, just buy something.
  - Security? Compliance? Ops?
- Define scope: Be vague
  - Real-time? Platforms? Log volume? Reports? Alerts? Usage?
  - Assume you are the only stakeholder

Worst practices

- Shortlist vendors:
  - Choose by initial price. Ignore modules, support, training,
  - Accept vendor TCO or ROI formula
  - Choose by relationship. We already use their AV or OS or IDS
  - Choose by Powerpoint

Worst practices

- Conduct POC
  - Don’t bother
  - Ignore the vendor completely
  - Let vendor dictate the POC
  - Don’t verify references

Worst practices

- Deploy
  - Don’t plan before the vendor shows up
    - Demand admin access at the last minute
    - Scramble to configure network/firewall
    - Use any old hardware or software
    - Surprise staff with the schedule
      - Announce training at the last minute
    - Ignore the vendor recommendations
      - What do they know anyway?

Worst practices

- Use
  - Don’t upgrade to new release
  - Don’t invest in support contracts
  - Ignore vendor provided best practices
  - Never provide training to the actual users
- Expand
  - Don’t designate a product owner
  - Donr check for changed needs or scalability

Final Thoughts -- Seriously

- Implementing Log Management is a typical IT project
  - Planning early and often is key
- Match your needs to product features
- Conduct a pilot, verify claims
- Befriend your enemy (vendor)

Contact

Download this presentation at:

www.eventtracker.com/itsac2011

ananth@eventtracker.com

Vendor Expo

Booth #408